AMENDED

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Samuel Morgan, being first duly sworn, hereby depose and state as follows:

Introduction

1. I make this affidavit in support of an application for a criminal complaint and arrest warrant charging Tushal Rathod ("Rathod"), year of birth 1980, with Wire Fraud, in violation of 18 U.S.C. § 1343, Conspiracy to Commit Wire, in violation of 18 U.S.C. § 1349, Money Laundering, in violation of 18 U.S.C. §§ 1956(a)(1)(B), and Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h).

2. The facts set forth in the Affidavit are based on my personal observations, my training and experience, information obtained from other agents, witnesses, and records obtained during the course of the investigation. Because I submit this Affidavit for the limited purpose of showing probable cause, I have not included in this Affidavit each and every fact that I have learned in this investigation. Rather, I have set forth only facts sufficient to establish probable cause to issue an arrest warrant for the individuals identified herein and to seize the bank accounts set forth herein. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

Affiant Background

3. I am a Special Agent of the Federal Bureau of Investigation (FBI) in Providence, Rhode Island, duly appointed according to law and acting as such. I have been employed with the Federal Bureau of Investigation (FBI) as a Special Agent since 2018. From July 2018 to October 2020, I was assigned to work counterintelligence matters in the FBI Washington Field Office. From October 2020 to January 2023, I was assigned to the FBI San Juan Field Office where I worked investigations involving complex financial crimes, including matters involving

fraud and theft of cryptocurrency. From January 2023 to present I have been assigned to an FBI Cyber Task Force, in the San Juan Field Office from January 2023-February 2024, and in the Providence Office from February 2024- present. I have conducted numerous complex investigations concerning computer crimes and fraud, including wire and mail frauds, intrusions (i.e., gaining access to a protected computer or computer network without permission), and the use of botnets (i.e., a group of computers controlled without the knowledge of the computers' owners). I have experience reviewing records related to computer crime and fraud, including Internet Protocol ("IP") address logs used by computers on the Internet, network access logs, and security programs. I also have experience debriefing defendants, witnesses, informants, and other persons involved in computer crime and fraud. I have personally conducted and have been involved in numerous investigations that included the execution of search warrants involving electronic evidence and have been involved in all phases of investigations of computer intrusions.

Overview of Rathod's Criminal Conduct

4. Based on a 2022 report to law enforcement made by a law firm in Rhode Island that had been the victim of a business email compromise ("BEC") scam, the United States began an investigation into Tushal Rathod and others. As part of that investigation, investigators obtained records from Google for tushal27@gmail.com via court order. They also obtained records from Apple, Inc. for the Apple iCloud accounts belonging to tushal27@gmail.com and kluvbb110011@gmail.com via warrants. In addition, investigators have obtained bank records from numerous financial institutions for accounts controlled by Rathod or individuals that he recruited into the scheme.

5. Rathod is a 44-year-old Legal Permanent Resident (LPR) of the United States. Rathod's current address is 108 Niblick Cir., Baldwinsville, New York, 13027, a residence that he purchased in February 2025. "Contract to Purchase" obtained from the seller's attorney indicates that Rathod purchased the home at 108 Niblick Cir. for $250,000 in cash.

6. Rathod incorporated two companies that he used as part of the scheme. He opened multiple business bank accounts under the name of these two companies, and he was a signatory on those accounts. He used these accounts to receive and launder fraudulent proceeds.

a. In 2016, Rathod registered T3 Telecom, LLC with the New York Department of State. According to the Department of State records that are publicly available online, T3 Telecom is a domestic LLC with a business address of 5 Avon Parkway, Apt.1, Liverpool, NY 13090. Publicly available information indicates T3 Telecom was a telecommunications company that did network testing and deployment of network devices.

b. According to records of Delaware Department of State that are publicly available online, TSV Telecom Constructions LLC was incorporated in 2021. Per its website, TSV Telecom Constructions LLC is an upstate New York-based telecommunications and civil construction firm. The address on the TSV Telecom Constructions LLC webpage is listed as 128 Via Serena, Rancho Santa Margarita, California, 92688, USA.[1]

7. Through review of financial records obtained via grand jury subpoena and other means, I learned that between April 2022, and June 2024, Rathod received over $1.7 million in suspected fraudulent proceeds generated through BEC fraud deposits and counterfeit checks. He

[1] As discussed in paragraphs 39-40, Kent Joy LLC was another company created and used as part of the fraud and money laundering scheme. Bank records obtained in this investigation indicated that Kent Joy LLC was also registered at 128 Via Serena, Rancho Santa Margarita, CA 92688. Kent Joy's bank account received fraudulent proceeds into its account and there was no apparent business income in the account.

received these funds into seven bank accounts at six different banks that he opened between January 13, 2022, and May 2024. Five of the accounts were in the name of T3 Telecom, LLC and one account was in the name of TSV Telecom Constructions, LLC. Through financial analysis of the account records, investigators learned Rathod purchased over $1.2 million worth of Bitcoin using fraudulent funds and sent it to external addresses.

8. At least three financial institutions contacted Rathod in 2022 regarding the fraudulent nature of incoming funds to Rathod's financial accounts.

a. In May 2022, Wells Fargo notified Rathod funds coming into his account were unauthorized and his account would be closed.

b. In late 2022, Rathod was contacted on multiple occasions by M&T Bank and informed that funds coming into his account were reported fraudulent. In response to the questions from M&T Bank Rathod emailed M&T a fraudulent invoice to justify the funds as legitimate income. The email was from November 28, 2022. The invoice Rathod provided to M&T Bank was shown to the victim who confirmed that the invoice was fraudulent. Rathod was later informed by M&T Bank that police reports were filed pertaining to additional funds received by Rathod in his M&T Bank account. Rathod stated he believed he was scammed. Rathod was asked for additional documentation regarding wire transfers. Rathod did not contact M&T Bank again after learning police reports had been filed, and Rathod did not provide additional documentation.

c. In December 2022, AmeriCU Credit Union advised Rathod by letter that they restricted certain services due to Rathod's receipt of fraudulent wires into his T3 Telecom account.

9. Accounts used by Rathod during the scheme are set forth in the subparagraphs below. In reviewing bank records for these accounts, a financial analyst working on this investigation observed some business activity in accounts that also received fraudulent funds. Based on my training and experience, I know individuals engaged in fraud schemes often open multiple bank accounts under business entity names to receive funds from victims, commingle victim funds with other seemingly legitimate funds, and then move them to other accounts in an effort to conceal the nature and source of the funds.

a. JP Morgan Chase ("JPMC") Acct. #2602 in the name of T3 Telecom, LLC was opened January 13, 2022, and closed July 25, 2022. A total of $677,786.02 was deposited into the account, of which $39,422 or approximately 5.8% appeared to be business income.[2]

b. JPMC Acct. #9397 in the name of TSV Telecom Construction, LLC was opened June 14, 2022, and closed July 22, 2022. There were no apparent legitimate business deposits made to that account during that time period; however, there were $122,428.20 in fraudulent proceeds deposited into the account.

c. M&T Bank Acct. #4453 was opened October 4, 2022, through January 31, 2023, in the name of T3 Telecom, LLC. A total of $253,462.81 was deposited into the account, of which $16,550 or approximately 6.5% appeared to be business income.

d. Coastal Bank Acct. #4866 was opened on November 28, 2023, in the name of T3 Telecom, LLC and records were reviewed though May 2024. During that time period, no legitimate business deposits were made to the account; however, there were $35,500

[2] The incoming funds were categorized as apparent business income based on the source of funds being various telecommunications companies, which matches the stated business function of T3 Telecom and TSV Telecom Construction, LLC.

in fraudulent proceeds deposited into the account. There was also a $85,000 attempted check deposit declined by Coastal Bank due to origin outside of the United States.

e. SECNY Account #1003 was opened on May 28, 204 in the name of T3 Telecom, LLC and records were reviewed through June 2024. During that time period, no legitimate business deposits were made to the account; however, an $85,000 check was deposited into the account on June 6, 2024. That check was later returned as counterfeit.

f. Citizens Bank account #2146 was opened on January 13, 2023, in the name of T3 Telecom, LLC and records were reviewed through July 2023. During that time period, four deposits were made to the account, three of which had no legitimate business purpose. The source of funds for the fourth deposit, an incoming wire in the amount of $37,950 on February 10, 2023, is unknown.

g. Wells Fargo account #4423 was opened November 4, 2016 in the name of T3 Telecom, LLC and records were received from January 2, 2019 through May 13, 2022. The account was closed on or about May 16, 2022, by Wells Fargo. Based on a cursory review of the records received, there was over $1.9 million deposited into the account during that time. Of that amount, there was at least one fraudulent deposit on April 27, 2022, totaling $27,422.

10. In addition to using his own business and personal bank accounts in furtherance of the fraud and money laundering scheme, Rathod recruited others to create businesses and open business bank accounts to be used to receive and launder fraudulent proceeds. Specifically, he recruited his girlfriend, Uncharged Coconspirator #1 (UC1), the user of the Apple iCloud Account associated with kluvbb110011@gmail.com, and more recently, between May and July 2024, Rathod recruited purported family members to assist in the scheme. Rathod facilitated his girlfriend's and family members' communications with the source of the fraudulent proceeds,

and as a result over $1 million additional dollars were deposited into accounts controlled by Rathod's girlfriend and family, although Citibank was able to recover $800,000 of those fraudulent funds.

Business Email Compromise and Money Laundering

11. One type of internet-based fraud scheme that is of particular relevance to this affidavit is a business email compromise ("BEC"). During a BEC, scammers obtain the login credentials of an email user of a business email account. Typically, the credentials are obtained during a "spearphishing" cyber campaign.

12. Using stolen credentials, the fraudsters log in to the business email account and then monitor the email traffic over the account to identify communications concerning upcoming financial transactions that they can insert themselves into (e.g., an upcoming wire transfer to pay a regular vendor that has issued an invoice for goods or services).

13. Sometimes, fraudsters install malicious software or "malware" to infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information is used to time requests or send messages so that accountants or financial officers do not question payment requests or request change-of-bank-account information. Malware also lets criminals gain undetected access to a victim's data, including passwords and financial account information. Next, scammers will register a domain that is similar to, but slightly different from, the domain used by the beneficiary of the upcoming transaction (e.g., john.kelly@exampleinc.com vs. john.kelley@examplelnc.com--where the lower case "I" in "inc" has been replaced with a lower case "L" or the name "Kelly" has been misspelled as "Kelley").

14. Another technique involves using a third-party service to send a spoofed email seemingly from the legitimate beneficiary of the upcoming transactions.

15. In either situation, the scammers then draft emails using the spoofed email account that provide purportedly "new" banking information where the upcoming payment should be sent. Lulled into believing they are dealing with an established and known company employees of the victim company will provide the "new" banking information to a financial institution when initiating the upcoming payment. In fact, the "new" banking information is information associated with a conspirator's bank account. In this way, the victim company transfers money to the fraudsters. Following transfers, money launderers rapidly deplete the fraud funds from the account of deposit by engaging in multiple financial transactions. As a result, by the time the fraud is discovered, usually the victim's money is gone and difficult to trace to the wrongdoers.

16. In my training and experience, I know that fraudsters and individuals who conduct BEC schemes often work with a vast network of money launderers to help them "clean" funds and then re-integrate the "cleaned" funds into the economy so that the funds can be used free from the taint of criminal activity. This allows the scammers to profit from their fraudulent conduct and to avoid getting caught. To these ends, scammers work with others to use, and recruit others to use, multiple bank accounts to move money in a series of convoluted transactions that makes it harder to identify the source of or who controls the funds. This is often referred to as "layering" or "funneling." The use of "money movement" bank accounts ("movement accounts") to layer or funnel fraud often works as follows:

a. A few days before or around the same time that the fraud scheme is being perpetrated, a money mover is recruited to open a movement account(s). Sometimes, a

movement account may be opened 60-120 days prior to execution of a fraud scheme so as to allow a "cooling off period" (banks more carefully scrutinize transactions made to newly-opened accounts, and sometimes banks place limitations on how soon after opening an account funds deposited to the account can be withdrawn).

b. The movement account(s) receive fraud proceeds, which are sometimes commingled with other funds.

c. Within several days to weeks, and following the direction of a person connected to the fraud, a money mover will engage in transactions with the funds in various ways—for example, by withdrawing large amounts of cash from the movement account (sometimes obtaining cashier's checks with those funds), or using checks, ACH/wire transfers, or debit cards to withdraw cash in order to redistribute the fraud proceeds to others. The funds are sometimes converted to and/or moved via cryptocurrency.

d. Often, the beneficiaries of the transactions are other movement accounts; these movement accounts in turn use the funds they receive to conduct additional financial transactions with the funds. The purpose of these transactions is to further obfuscate the connection between the source of the funds and the perpetrators of the schemes.

e. After the funds are depleted, a money launderer will often close the movement account(s). Sometimes, banks will freeze or close accounts they come to suspect are being used to launder funds from fraud or other criminal activity.

Rhode Island Law Firm Becomes a Victim of a BEC and Rathod Launders the Proceeds

17. In or about June 2022, a Rhode Island based real estate law firm (Victim 1) reported to the FBI that they were victims of a fraudulent email scheme in which they lost approximately $163,298. Victim 1 and an employee at Northpointe Bank had previously

corresponded via email regarding real estate matters. On or about April 28, 2022, Victim 1 received an email purporting to be from the same employee at Northpointe Bank. The email correspondence directed Victim 1 to send funds to an account supposedly belonging to a Mortgage Company, Carrington Mortgage, associated with a valid real estate transaction. Further investigation revealed the email sent to Victim 1 with financial account details was sent using email spoofing website "hxxps://emkei[.]cz." The email appeared to be from the Northpointe Bank employee Victim 1 had previously engaged with at the bank, however, the bank's email address was used fraudulently via email spoofing.

18. The spoofed email instructed directed Victim 1 to send the funds to JPMorgan Chase account ending in #2602 ("Account #2602"). Pursuant to these instructions, on May 4, 2022, Victim 1 wired $163,298 to Account #2602. Subsequently, a user of Account #2602 wired a total of $100,000 to a Silvergate Bank account ending in #8012 ("Account #8012"), where they were sent to Gemini cryptocurrency exchange, converted into Bitcoin and withdrawn to multiple Bitcoin addresses. At that time, Silvergate Bank served as an intermediary that allowed customers to deposit and withdraw United States dollars to and from cryptocurrency accounts held at Gemini Trust Company, LLC, a cryptocurrency exchange.

19. JP Morgan Chase records for Account #2602 show that Account #2602 was in the name of T3 Telecom, LLC. JPMorgan Chase records for Account #2602 also showed that Account #2602's user data included email address tushal27@gmail.com. JPMorgan Chase records indicated Account #2602 was accessed by a user using tushal27@gmail.com via an Apple iPhone on multiple occasions before, on, and after May 4, 2022, the day of the fraudulent wire from Victim 1.

20. Silvergate Bank records for Account #8012 show that Account #8012 was registered to Gemini Trust Company, LLC, a cryptocurrency exchange that was affiliated with Silvergate Bank. Based on Silvergate Bank records for Account #8012, $100,000 was then deposited into Gemini Trust Company, LLC account ending in #2259 (Account #2259), in the name of T3 Telecom, LLC, with the primary user listed as Tushal Rathod.

California Becomes a Victim of a BEC and Rathod and Others Launder the Proceeds

21. An FBI Investigation in Los Angeles, California was initiated in February 2023 based on BEC on Victim 2, California credit union. Victim 2 was fraudulently induced to send approximately $8 million to bank accounts controlled by others, including a resident of Minnesota, Uncharged Coconspirator #2 (UC2). The fraudulent transfers occurred in late January 2023. Of the fraudulent funds, approximately $4.2 million in fraudulent funds were sent to UC2's financial accounts at Bank of America in two transactions in January 2023.

22. After the transfer of the fraudulent funds to UC2's Bank of America account, the funds were used to purchase a cashier's check for $990,000. On February 2, 2023, this cashier's check was deposited into Citizens Bank account ending in 2146 ("Citizens Acct. #2146") and held in the name of T3 Telecom, LLC. Citizens Acct. #2146 was controlled by Rathod.

23. Rathod subsequently sent $900,000 to Gemini Acct. #2259 on February 9, 2023, keeping $90,000 of the fraudulent funds for himself. [3] On February 10, 2023, Rathod purchased approximately 20.18 and 20.16 Bitcoin in two transactions, totaling $900,000. Rathod then sent 20.18 and 20.16 Bitcoin in two transactions on February 10, 2023, to an unidentified recipient. Based on my training and experience, Rathod and UC2 were laundering the fraudulent proceeds

[3] Information provided by Citizen's Bank indicated that the $990,000 check deposited into Rathod's Citizen Bank Acct. # 2146 and the subsequent $900,000 wire transfer out of the account transited servers located in East Providence, Rhode Island.

through their accounts, with Rathod ultimately converting a portion of the funds to Bitcoin and sending to an unidentified recipient.

Rathod and UC2 Discuss the Receipt and Disposition of Fraudulent Funds

24. Records obtained from Google revealed Rathod and UC2 exchanged email communications on multiple occasions from 2023-2024. Rathod asked UC2 on one occasion if he was "still doing business with Pedro?" and UC2 replied from email address leon@hughadsdoctor.com, "How are you? Yes, Indeed." Rathod inquired if UC2 was, "having any issues on getting accounts closed?" UC2 replied, "Bank of America was my biggest challenge. Now I have challenges with Merchant since they constantly asking for more information before proceeding with transactions." Later in the conversation, in December 2024, Rathod stated "Oh man. I feel you. It's difficult doing this business but it's got a lot of good money you can make." Rathod later stated, "Trust me man. I have been going through the same. Every time payment comes the account gets frozen. I have lost many accounts also. The worst part is HOD doesn't believe me when I say account is frozen and money is going to get sent bank."

Witness 1 Reports Observing Suspected Money Laundering Transactions on an Apple iPhone That Rathod Gave to Their Child

25. In or about March 2024, Witness 1, a woman who was previously in a relationship with Rathod and is the mother of Rathod's six-year-old child, made an IC3 complaint to the FBI under another person's name. In the complaint, Witness 1 accused Rathod of money laundering. I interviewed Witness 1 on or about April 8, 2024. Witness 1 said that she was previously employed by Rathod at T3 Telecom. Witness 1 stated T3 Telecom operated from 2016-2020, then Rathod started TSV Telecom Construction in 2020. Rathod asked Witness 1 to open multiple financial accounts and stated he was involved in some type of "bank

hopping." Witness 1 stated Rathod switched banks often because local banks closed his accounts often.

26. According to Witness 1, Rathod provided their child with an Apple iPhone at an unspecified time. Witness 1 said that she took the phone from her child after discovering sexually explicit adult content in the Photos application on the phone. When Witness 1 took the phone, she also saw screenshots containing financial information. Specifically, Witness 1 saw screenshots from multiple financial institutions in which there were attempted deposits of large sums of money into various bank accounts. The screenshots appeared as if the deposits were not accepted by several banks. In addition, Witness 1 also discovered screenshots of chats in foreign languages between Rathod and others referencing cryptocurrency transactions, and other screenshots of Rathod sending cryptocurrency transactions. According to Witness 1, the email account associated with iPhone's Apple ID was tushal27@gmail.com.

27. Shortly after my conversation with Witness 1, Rathod attempted to contact me via phone multiple times via phone calls and texts despite Witness 1 telling me that she would not inform Rathod of our conversation. Rathod texted me the question, "Are you tapping my phone conversations?" I returned his missed calls and Rathod asked who I was and where I was calling from. I responded that I was "Sam" calling from my cellphone and that I had a few missed calls and texts from this number. Rathod stated Witness 1 told him she spoke with me, told him that his phones were being tapped, and provided my contact information.[4] I responded that I had no clue what he was talking about and that I was not tapping anything or knew what that meant. Rathod then ended the conversation by saying, "ok thanks."

[4] I have also reviewed a report from the Baldwinsville Police Department from 2024 in which the officer said that Witness 1 told him that the FBI had contacted her to let her know that Rathod opened credit cards in her name. I did not have a discussion with Witness 1 regarding Rathod opening credit cards in her name.

28. Based on my subsequent review of text conversations between Rathod and Witness 1 obtained through court authorized warrants as described in paragraph 30, I learned that Rathod has used multiple phones in addition to the iPhone described above. For example, on May 1, 2022, approximately three days prior to the theft of funds from Victim 1, Rathod sent a text to Witness 1 that stated:

"I have put my boundaries (sic) and the first step was to get another phone line. So this line and this number is only for business and other bs. The other number is strictly for myself when I'm hanging out with my son or friends."

Rathod then sent a photo of a green iPhone to Witness 1 as well as a link to a Samsung Galaxy Z Fold5 256GB cellphone. Rathod stated, *"I got this for this line and for business."* Witness 1 replied, *"So now you have two phones at all times lol,"* to which Rathod stated, *"Yup"* and *"Only when I'm off I won't take the business phone."*

Conversations Between Rathod and Other Co-conspirators

29. On May 6, 2024, as well as on August 22, 2024, I served Apple, Inc. with a search warrant signed in the District of Rhode Island requesting account information pertaining to the Apple iCloud account belonging to tushal27@gmail.com. I also served Apple a search warrant signed in the District of Rhode Island requesting account information pertaining to the Apple iCloud account belonging to kluvbb110011@gmail[.]com and believed to be used by UC1.

30. Among the data reviewed to date pursuant to the search warrants, there were multiple WhatsApp and iMessage conversations in which the user of the Apple iCloud account belonging to tushal27@gmail.com, believed to be Tushal Rathod, discussed the receipt and sending of funds and the opening and use of financial accounts at multiple institutions, to include Gemini Trust Company, LLC. Rathod had extensive conversations about the receipt and transfer

of funds that the investigation has revealed are the fraudulent proceeds of BEC. These conversations were between Rathod and the following WhatsApp contacts: "PEDRO Chang" ("Pedro"),[5] phone number 202-922-6617, and "Keith Rayonk" ("Keith") with phone numbers 915-765-6823 and 940-437-1661. In addition, there were numerous conversations with UC1, phone number 315-506-8322, a woman I believe to be Rathod's girlfriend that he involved in the scheme.

31. The excerpts identified below are not exhaustive and only a portion of all conversations identified from the Apple iCloud search warrant records for the Apple iCloud account belonging to tushal27@gmail.com that appear to relate to Rathod's receipt and laundering of fraudulent proceeds:

a. Rathod had text conversations with Keith Rayonk, phone number +1 (940) 437-1661, beginning on November 19, 2021, and continuing until February 7, 2022. On November 19, 2021, "Keith" contacted Rathod *"For Job Inquiry."* They discussed what type of "accounts" Rathod had, and Rathod forwarded his name and company *"T3 Telecom LLC,"* along with address 181 Blackberry Rd., Liverpool, NY 13090. Keith replied with the following:

Tushal,

This is to acknowledge receipt of your information and to inform you that it has been reviewed. You have been approved to be our company's Representative in North America by the Board of Directors and a file has been created with the accounts department to that effect. We hereby attach the Memorandum of Understanding to this email. You are to sign and return via email upon receipt. We want to use this medium to reaffirm our pledge to this relationship as further confidential information would be sent to your attention afterwards. Do acknowledge receipt of this mail.

I await your reply.

[5] This individual identified himself as "Pedro Cheng" as elaborated in paragraph 31d but he was listed as "PEDRO Chang" in Rathod's WhatsApp contacts.

We look forward to your reply,
Sincerely,
Keith Leatherwood
Consultant"

b. On January 5, 2022, Keith asked *"How are you doing?"* and *"I will forward you confirmation soon"* and *"I just want to make sure you are available and active."* Rathod replied, *"ok."* Based upon my experience and review of these text messages, when Keith asked Rathod whether he was "available" and "active," he was referring to having active bank accounts to be used to receive and launder fraudulent funds.

c. On February 8, 2022, Rathod received a text from 19157656823 and the individual texting from this number identified himself as "Keith from Rayonhk." Later, on February 17, 2022, Keith stated *"Informations received and has been stored on company's data base. You will now be added to the Sales Representatives WhatsApp group by the Head Of Department in charge of fixing clients and jobs according to jurisdictions. Thank you"*

d. In February 2022, Pedro stated the following to Rathod:

"Good day Mr Tushal Rathod,

My name is Pedro Cheng of Rayonhk Construction Company, HOD in charge of all jobs going out to every Sales Representatives and I welcome you to this WhatsApp platform.

I will ask for your total dedication and cooperation as we embark on this journey for growth in business.

Note; Kindly be patient as we expect payment from the client assigned to you as it should be sent out anytime from now.

Please have a good evening.

Pedro".

e. On March 30, 2022, Rathod asks Pedro, *"Hope none of this will get me in any trouble?"* to which Pedro replies, *"No no troubles Mr. Tushal."* [6]

f. In late March 2022, Pedro and Rathod discussed incoming payments to Rathod, and Pedro specifically asked Rathod if he linked his bank with Gemini. Rathod responded, *"I will call you later in the afternoon. So we can do Gemini."*

g. Pedro continued to follow up throughout April 2022 by asking Rathod if his Gemini account was operable. Rathod replied multiple times stating that he was waiting on Gemini verification. On or about April 21, 2022, Rathod told Pedro that Gemini was working.

h. Throughout late April 2022 Rathod and Pedro discussed Rathod's "*salary"* and incoming payments to Rathod's account. On April 27, 2022, Pedro told Rathod the following:

> *"So couple of funds has been made out to you"*
>
> *"One just got confirmed"*
>
> *"PFO220427315938*
> *Amount: $27,422*
> *Wire coming from Pentagon Financial Credit Union*
> *Wire Name: Jeannette Gwendolyn Andrews Thompson".*

Pedro then stated:

> *"The second is about 28k"*
>
> *"This is the trial deposit before the bigger amounts".*

[6] The Apple iCloud search warrant records for the Apple iCloud account belonging to tushal27@gmail.com also show that in December 2023, Rathod states "I am not sure what's going to happen to my son if I get in trouble," to which Pedro replies "You are getting into any trouble." Rathod also states on December 5, 2023, "Mr Pedro I don't want to work with 5%. I can make that money legally and without getting the accounts jeopardized," when discussing the salary percentage Rathod receives from the payments that come into his financial accounts.

i. On Thursday April 28, 2022, Rathod messaged Pedro, *"Just received the money on Gemini."* Rathod later confirmed**,** *"21,150 transferred"* to Pedro. Pedro also sent the Bitcoin address "bc1qqyfcdj6xmrww85ua65qk90urtzju8cqum4fy2y" to Rathod multiple times throughout this conversation. Bank records provided by Gemini identified a deposit of $21,120 into Gemini account #2259 and a subsequent purchase and transfer of Bitcoin in the amount of approximately .55297025 BTC, approximately $20,805.31 minus a fee from Gemini of $314.69, to the Bitcoin address identified by Pedro. Notably, on the same date of April 28, 2022, Victim 1 received a spoof email purporting to be from Northpointe Bank directing Victim 1 to send funds to an account supposedly belonging to Carrington Mortgage, but which was actually a bank account registered to Rathod. Based on my experience, reading of and timing of the text messages between Rathod and Pedro, and review of JPMC Acct. #2602 records registered to Rathod, the "bigger amounts" that Pedro referenced appear to be the anticipated wire from Victim 1 in the amount of $163,298.

j. On April 29, 2022, Rathod stated, *"They haven't made any payments."* This was the last message recovered in the WhatsApp conversation between Rathod and Pedro until November 2023. Based upon my experience and review of JPMC Account #2602, *"payments"* is believed to be the payment from Victim 1 in the amount of $163,298 that was anticipated to be wired into Rathod's account, JPMC Account #2602, and was later wired into this account on May 4, 2022, by Victim 1.

32. In reviewing the Apple iCloud warrant results for the account associated with tushal27@gmail.com, I noted that there was a break in Whatsapp conversations between Rathod and Pedro, and Rathod and Keith, from April 30, 2022, to November 2023, even though he continued to receive fraudulent proceeds during this time. This could be the result of Rathod's

use of different cellphones. Based on my training and experience, I know that criminals engaging in fraud often use multiple cellphones to communicate and conduct fraudulent transactions in order to avoid detection by law enforcement. I also know that Rathod specifically messaged Witness 1 about his use of more than one cell phone.

33. Although the specific transactions in which Victim 1 lost funds occurred during the period of time in which Rathod does not have conversations with Pedro backed up to his iCloud for tushal27@gmail.com, the conversations from the days and weeks leading up to Victim 1's loss involve the same pattern of activity used to move Victim 1's funds. That is, the conversations leading up to the break in backed up communications received from Apple reference the transfer of funds to a bank account owned by Rathod, movement of the funds to Gemini, purchase of Bitcoin, and transfer of Bitcoin to an address provided by Pedro.

34. In January 2024, Pedro asked Rathod, *"Do you have any construction account at the moment? For 1.5M job.*" Rathod stated *"yea, TSV, with Bluevine."* Pedro asked, *"Can Bluevine take that amount?"* and Rathod replied with, *"yeah."* Pedro stated, *"I don't want any f***ups [expletive in original] this time."* Rathod replied, *"Mr Pedro. My accounts don't get f****ed [expletive in original] up like that. As I said before my business are old enough and nature of the business is legit to have transactions like this."* Based on my training and experience, Rathod indicated his accounts had apparently legitimate history and usage, making them easier to move illegally obtained funds through the account without the Bank compliance department taking action to stop the illegal activity.

35. In a conversation between Pedro and Rathod on January 12, 2024, Rathod stated, *"Keith reached out saying there's a payment coming to those Bluevine accounts. I just don't understand if you don't trust me and call me a thief then why are we doing this? Don't get me*

wrong if there's a payment coming I will deliver it but just doesn't make any sense to me." On February 1, 2024, Rathod stated to Pedro *"Hello Mr Pedro. I'm not sure about this but Keith keeps asking us to open different bank accounts and like I told you last time he almost got me in trouble."* On February 18, 2024, Rathod stated to Pedro, "*Keith said payment is coming on Kayla's account. I thought you said it's coming on my account before hers?"*

36. The recovered conversations between Rathod and Pedro resumed in November 2023. Throughout February and March 2024, Pedro and Rathod discussed incoming payments to Rathod's accounts from unspecified clients of Pedro's. On March 29, 2024, Rathod told Pedro, "*I have Bluevine we can use for now*." Per open-source information, Bluevine is a financial technology company that provides banking services through a partnership with Coastal Community Bank. On April 1, 2024, Rathod told Pedro, "*We have BOA accounts now*," likely referring to Bank of America accounts based upon my experience. On April 3, 2024 Rathod stated, "*Is it worth having this accounts? 4 accounts got closed next day the payment came through*."

37. Between May and July 2024, Rathod sent multiple financial accounts to Pedro. Rathod asked for updates regarding the status of additional payments. On May 15, 2024, Rathod messaged,*"Mr Pedro. Are we every going to receive any real payments I really need you to be honest with me man? Should I close the BMO account? It's my nephews account and I don't want to get him in trouble."*

38. On May 26, 2024, Rathod stated, *"Also my nephew is working on opening a business and bank account and the good thing is that he is in California so we can have multiple crypto accounts."* On May 28, 2024, Rathod stated *"Me Pedro. If I get you more people and accounts is it guaranteed that the business is going to get busier and will have regularly*

payments coming?" to which Pedro replied *"Yes you sure will."* Rathod replied *"Ok. I'm just going to give you family members they are trust worthy. And I have full control over them."* Pedro replied, *"OK Perfect,"* to which Rathod stated *"I have my other nephew who's going to register for business also."*

39. On June 19, 2024, Pedro asked *"Please can you have them put in some amount in all of these account."* Over the course of the conversation from May to July Rathod sent Pedro information on two Bluevine accounts in the names of TSV Telecom constructions LLC and T3 Telecom LLC, one Bank of America account in the name of Kent Joy LLC, and one Chase bank account in the name of Betiman Enterprise LLC.

40. During this time, Rathod had a group chat in WhatsApp called "*Investors*." The members of the group chat were Rathod, "Fauwaz Shakil" using phone number 1-949-350-7661, "Arbaaz" using phone number 1-949-259-3609, and one hidden user. The chat is in a mix of English and Swahili. The participants discuss the status of various bank accounts and payments to those accounts. For example, on June 4, 2024, Fauwaz Shakil sent account information for a CitiBank account in the name of Kent Joy, LLC. Shakil and Arbaaz both sent usernames and passwords for the financial accounts they provided Rathod, and Rathod asked on June 5, 2024 if they could please keep all the passwords the same.

41. Pedro sent Rathod a message on June 21, 2024, and stated, "*Also please the citi bank for Kent would be used for 1m kindly add that account up and work on it. I'll need to show you how we would pull the funds out."* Rathod then forward the exact same message, in English, to the *"Investors"* group. Shakil replied "*Citibank wamesema kwamba watanipa update 1-2 business days"* **[Translated via Google Translate**: *"Citibank has said that they will give me an update in 1-2 business days"].*

42. Three days later, on June 24, 2024, a Texas company was the victim of a BEC scheme in which they sent $1,045,255.80 to the incorrect recipient. They were fraudulently induced to send the funds Shakil's Kent Joy LLC account at Citibank. Records for that account indicate that $1,045,255.80 came into the account on June 24, 2024. Two cashier's checks were purchased on June 25, 2024. One check was for $100,000 and one was for $105,000 both payable to Kent Joy LLC and deposited into an account at JP Morgan Chase. Rathod followed up in the "*Investors*" group chat and stated "*@19493507661 wapigie citi bank angalia zile hela inakuwaje"* **[Translated via Google Translate: "**@19493507661 call Citi Bank to see how the money is going."] IP records from CitiBank for the account reflected multiple logins from Charter Communications infrastructure based in Baldwinsville, New York, where Rathod resides.

43. Rathod stated to Pedro on June 25, 2024 *"You want him to deposit that to chase correct?"* and subsequently on June 28, 2024 "*Good morning Mr Pedro. Our online access for chase got locked because of multiple attempts from NY but the account is still good. Soon as my nephew wakes up I will have him call them and check if the 100k is clear and we can complete the transaction today."*

Rathod's and UC1 Discuss the Receipt and Laundering of Fraudulent Proceeds

44. From May 21, 2022, to May 3, 2024, Rathod had extensive text conversations with phone number +1-315-506-8322, believed to be used by UC1. JP Morgan Chase records for an account opened in the name of TKVO Enterprise LLC c/o UC1 identified phone number 8322 and email address kluvbb110011@gmail.com, and were provided in account opening documents. In the interview conducted in April 2024, Witness 1 informed FBI Agents that Rathod was currently dating and working with UC1. The first identified discussions between UC1 and

Rathod of "payments" received by Rathod were on June 21, 2023, when Rathod stated, *"And I got some of my payments today lol."* Rathod later stated on August 21, 2023, *"So we can provide information to the client and they can set you up for some payments this week."* In September 2023, UC1 stated to Rathod, "*Tushal I'm over this whole thing. It's alll a scam.*"

45. UC1 and Rathod discussed their respective conversations with Pedro, and on multiple occasions UC1 sent Rathod screenshots of her conversations with Pedro. Based upon my experience and reading of the subsequent messages between Rathod and UC1 and between UC1 and Pedro as described below, UC1 was working with Pedro to launder funds. Examples of the messages between UC1 and Pedro below include Pedro telling UC1 on or about October 16, 2023, that, *"Payment has been scheduled to be sent to your account,"* and UC1 telling Pedro on or about Thursday November 9, 2023, that she *"opened a key bank."*

46. In addition, the messages also revealed that Rathod and UC1 planned to take money from the account used to launder the funds without Pedro knowing and then tell Pedro that the account was compromised. On November 10, 2023, Rathod stated, *"I kinda want to f*** [expletive in original] them up before we close that account by getting a payment them withdraw cash and close the account. What do you think?"* UC1 replied, *"There's not gonna be a payment coming tushal."* Rathod replied *"there is."*

47. On Saturday November 11, 2023, UC1 texted Rathod and asked, *"We stealing this money?"* Rathod replied, *"Call."* On Tuesday November 14, 2023, Rathod asked UC1, *"Did Pedro get back to you?"* UC1 replied with a screenshot of her conversation with Pedro in which he said to UC1 that he would give her an "update" and that he was still waiting on a "project."

48. In a text conversation between Rathod and UC1 on November 17, 2023, UC1 stated, "*If this whole Thing Keith and Pedro put into scamming people They'd probably make some Real Money*."

49. In text messages between Rathod and UC1 in November 2023, they discussed counterfeit checks from Keith. UC1 stated, *"Keith said he is mailing me a check but we know how that works."* Rathod replied *"Don't deposit any checks you receive from them. Call the bank it came from verify the funds then do it."* Later, on November 18, 2023, UC1 told Rathod that she was waiting on a check from Keith to which Rathod responded, "*Lol. Don't depend on that check too much. They never go through.*" UC1 said, **"***Scam lol*" and Rathod responded, "*What is not scam?*" UC1 said, "*This check.*" Rathod stated, "*Trust me I know how this whole thing works lol. Watch once you receive the check they will ask you to deposit from the atm. The checks don't work.*" UC1 later clarified that the check she was referencing above was not from Keith but from an unrelated account.

50. Later in the conversation on November 21, 2023, UC1 stated, *"I got a check from Keith"* and *"It's the same as yours."* UC1 then sent Rathod an image of the check. UC1 later stated to Rathod, *"I found my Key Bank card I could do it there"* to which Rathod replied, *"No. Don't F*** up that account. It's not safe to do so."* UC1 stated, *"I just told him it's fake and idw it*" and Rathod replied *"Yeah. He's pushing me to deposit that and I told him idc what he wants. I will do what's right for me."*

51. On December 1, 2023, Rathod texted UC1, *"Can you send me a screenshot of your key bank?"* and *"Pedro said a payment had been made."* UC1 then sent a screenshot of her Key Bank Accounts ending in -2229 and -8414.

52. Rathod continued to follow up regarding a potential payment to UC1's account, eventually stating, *"99,950,"* and *"amount."* UC1 later sent a screenshot to Rathod showing a balance in her accounts of $99,955.79 with the text, *"Tushal I'm shitting my pants."*

53. Between December 1 and December 2, UC1 and Rathod exchanged text messages, and UC1 sent Rathod a screenshot of her conversation with Pedro requesting her 10% cut from the payment. UC1 then texted Rathod, *"I say we take this whole thing and bounce."* Based upon my experience and reading of the text messages, UC1 was referring to stealing the fraudulently obtained funds.

54. On Sunday, December 3, 2023, Rathod texted UC1, *"Hey. Call the bank in the morning and see if they can get 50k in cash ready for you. And the rest wire on this account below."* Rathod included a screenshot of his Bluevine Acct. # 4866. Rathod then stated, *"25k on each envelope,"* and *"Tell Keith and Pedro your account is compromised tomorrow but say that after 11:30."* UC1 replies, *"K"* and *"Got it."* Rathod then stated, *"Once you go to the bank take a picture from the outside and send it to Pedro around 11 and say I'm at the bank getting the transaction done"* and *"and take 45 min to an hour and just text them hey the bank said account is locked."* UC1 replied, *"K."* Rathod replied, *"Don't mess this up if you want to make more money."*

55. On Monday, December 4, 2023, UC1 texted Rathod, *"Send me an email with the wire and routing number along with the invoice number from your T3 email so it looks legit when I'm there."* Rathod replied, *"So when you go there they will only ask you for the routing and account number" "Put invoice #1004,"* and *"You have to tell them to put that invoice number on the notes."* UC1 replied, *"Ok send me the wire number, routing and invoice number*

w company name so I can screen shot it now." Rathod replied with a screenshot of the Bluevine account.

56. Rathod and UC1 discussed how she should remove the fraudulent funds from the bank. UC1 said that she would withdraw "*50k. 25 in each envelope. I'm going to wire 35,500 and leave 4,433.79 in the account*." Rathod said, "*Perfect.*" UC1 indicated during this exchange that she was nervous, and she said, "*Idw wire too much and make it look suspicious*." At one point, UC1 said, "*Dude, idk this is risky business*" and Rathod responded, "*The next wire is for 124k.*" UC1 said that she did not want to get arrested by the FBI.

57. Keybank records for UC1's account opened in the name of TVKO Enterprise, LLC on November 1, 2023 reflected the December 1, 2023, $99,950 deposit described above. This deposit was the result of fraud on a victim, Alpha Settlement Services ("Alpha"), a full-service title company in Pennsylvania. Alpha reported having received a $100,000 cashier's check related to the purported sale of a home, of which $99,500 ($100,000 minus a $50 wiring fee) was later wired into UC1's Keybank account.

58. After wiring the funds to UC1's account, Alpha learned that the $100,000 check that it had received was counterfeit. A representative from Alpha reported that Alpha was contacted by an individual purporting to be a client. This supposed client stated that they were purchasing a home and provided a $100,000 cashier's check from Scotia Bank in Canada. The client provided Alpha with a fully executed purchase agreement and the cashier's check, which Alpha deposited on November 22, 2023. On November 30, 2023, Alpha was notified that the home purchase agreement had been terminated. The client sent Alpha Settlement Services a fully executed termination agreement and requested their funds back. On November 29, 2023, Alpha attempted to wire $99,950 ($100,000 minus a $50 wiring fee) to a financial account held at

Boeing Employee's Credit Union. That financial transfer was unsuccessful. On December 1, 2024, Alpha then successfully wired the $99,950 to UC1's account as identified above. On December 5, 2023, Alpha Settlement Services received notice the initial check of $100,000 was counterfeit.

59. Prior to Alpha's discovery of the counterfeit check, on December 4, 2023, UC1 initiated the following cash withdrawals at Keybank branches:

- $10,000 cash withdrawal at the Keybank Baldwinsville branch, 10 E Genesse St, Baldwinsville NY, at 9:53 AM;
- $20,000 cash withdrawal at the Keybank Liverpool branch, 301 Second Street, Liverpool, NY, at 10:25 AM;
- $10,000 cash withdrawal at the Keybank Great Northern branch, 3935 Route 31, Liverpool, NY at 10:47 AM;
- $20,000 cash withdrawal at the Keybank Great Northern branch, 3935 Route 31, Liverpool, NY at 11:17 AM.

60. On December 4, 2023, $35,500 was wired from UC1's Keybank account to a Coastal Community Bank account belonging to T3 Telecom and controlled by Rathod. On December 5, 2023, $35,000 was sent to Rathod's SECNY Federal Credit Union account via ACH transfer. On December 6, 2023, Rathod withdrew $10,000 in cash from his SECNY Federal Credit Union account. On December 8, 2023, Rathod withdrew $16,000 in cash. The funds were further drawn down via Zelle transfers and retail purchases.

61. Pedro followed up with Rathod throughout December 2023 and January 2024 inquiring about the funds. Rathod told Pedro the bank recalled the funds and that the bank put UC1's account on hold. Pedro stated on multiple occasions that UC1 had the funds. Specifically, *"He payment made to Kayla was never refunded,"* and *"She has the funds"* on December 18, 2023. Rathod replied, also on December 18, 2023, and stated, *"she has no access to the*

account," and "The bank has put a hold and will be refunded when they close the claim." Rathod and Pedro continue to argue in January 2024 regarding Kayla's actions and the status of the payment. The investigation has not revealed any payments made to Pedro from the original $99,950 deposit to UC1's account.

Conclusion

62. Based on the above activities conducted by Rathod, including the continued receipt and sending of fraudulently obtained funds over multiple years, providing of a fraudulent invoice to bank to justify his receipt of fraudulent funds, discussion of his activities and acknowledgement of the fraudulent funds he received, and other activities outlined, I submit there is probable cause to believe that from in or about November 2021 through June 2024 Tushal Rathod committed Wire Fraud, in violation of 18 U.S.C. § 1343, Conspiracy to Commit Wire, in violation of 18 U.S.C. § 1349, Money Laundering, in violation of 18 U.S.C. §§ 1956(a)(1)(B), and Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h).

I declare that the foregoing is true and correct.

Samuel Morgan
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Sworn telephonically and signed electronically

June 16, 2025
Date

Judge's signature

Providence, Rhode Island
City and State

Patricia A. Sullivan, USMJ
Patricia A. Sullivan, U.S. Magistrate Judge